The Importance of User Behavior Analytics for Cloud Service Security

ORACLE CLOUD

To combat modern security threats, many enterprises are turning to security solutions that leverage user behavior analytics (UBA). By analyzing user behavior and forming a baseline definition of normal, these solutions can notify IT administrators when deviations occur.

The Need for New Ways to Protect Data

Traditional security measures based on protocol analysis and virus signatures continue to be part of every enterprise's defense system. However, these solutions are more applicable to legacy threats than the modern threats designed to target specific enterprises. Traditional solutions alone simply cannot keep up with the increasing sophistication of today's attacks and hackers. Nor can they cope with savvy users who, for sake of productivity and convenience, often attempt to bypass existing security measures and company policies. Traditional security measures also do very little to detect internal threats which are becoming an increasing concern for many enterprises.

To improve security for both cloud services and traditional IT, many enterprises are implementing security solutions that analyze user behavior. Rather than focusing solely on quickly identifying attack objects such as viruses and malware or beating the hackers to the punch with early discovery of vulnerabilities in operating systems or browsers, these UBA solutions focus analysis on actions performed by particular users, forming a baseline of normal behavior and continuously monitoring for deviations from the accepted norm.

REASONS FOR IMPLEMENTING A USER-BASED SECURITY SOLUTION

- Modern attacks may come from internal, privileged accounts that are difficult to detect.
- Modern threat targets may be many low profile users, rather than a few top executives.
- A lack of segregated access—either physical or virtual—makes it difficult to secure cloud environments.

Importance of User Behavior Analytics in Modern Security

Security solutions leveraging UBA have been around for years. There are however, significant reasons why UBA is becoming a critical component of every enterprise security solution, especially as companies migrate their infrastructure and applications to the cloud.

Modern Threat Behaviors

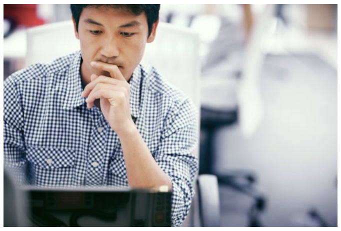
Legacy viruses and malwares are often identified by unique signatures. Some attacks can be identified by communication signatures such as those used in command-and-control malwares. Modern attacks, however, can evade traditional security measures by first creating a backup privileged account or by gaining additional privileges for an already compromised account. With the additional privileges, the hacker can perform various operations without raising any alarms. They can also defeat the security measures by simply turning them off.

One such threat behavior was highly publicized for causing a company to ultimately close their doors. After gaining access to an enterprise's Amazon Web Services (AWS) environment, the hacker first created a backup privileged account. Once the enterprise attempted to lock out the hacker following a ransom demand, the backup account was used to wipe out the company's entire cloud environment. A security solution leveraging UBA would have alerted the IT administrator of anomalous behavior such as account privilege changes or the creation of unauthorized privileged accounts.

Modern Threat Targets

Traditional security measures focus on securing high profile users. Executives, finance, and sales teams are a few of the groups that readily access highly valuable data. It is no surprise that they are most commonly targeted by traditional attacks to steal company and customer data. Modern attacks, however, often target these groups indirectly by first gaining access through other lower profile users. Once the hackers gain access to the enterprise network and resources, they can easily navigate the network to compromise other accounts and ultimately gain access to sensitive data.

A well-publicized attack on a national retailer started out as a breach on a low profile user. Once in the network, the hacker was able to bypass many of the installed security measures and steal millions of credit cards and other sensitive information. A security solution leveraging UBA would have detected a user attempting to gain access to confidential information even from within the network. In fact, a robust UBA solution can alert IT administrators of risky users—prime candidates for an attack—before accounts are compromised, arming the enterprise with predictive security.



Modern hackers often target high profile executives indirectly by first gaining access through other lower profile users. Once the hackers gain access to the enterprise network and resources, they can easily navigate the network to compromise other accounts and ultimately gain access to sensitive data.

Lack of Segregated Access

IT administrators accustomed to managing on-premises security often restrict access to the security appliance configurations. Administrative access is often segregated from other networks with unique requirements such as direct appliance connection or use of VPN. Of course, the appliances are secured from physical tampering behind locked wire closets. Unfortunately, many IT administrators lose these security precautions with the adoption of cloud services; there is no longer any perceived network separation, physical separation, or unique login procedures.

Losing the controlled administrative access the IT teams are accustomed to can represent a significant void in the security posture. UBA solutions fill this void by acting as another layer of security beyond simple credentials. By continually assessing the normal behavior of users, any deviations—including upgrading user privileges, accessing sensitive security settings, and changing security settings—can alert the IT administrator.

User Behavior Analytics in Oracle CASB Cloud Service

Oracle CASB Cloud Service addresses the visibility and security challenges enterprises face in cloud service environments such as AWS, Salesforce, MS Office 365, and Google Apps. Included in all Oracle CASB Cloud Service solutions, UBA capabilities analyze activities in individual, business-critical cloud applications as well as activities spanning multiple applications. With it, enterprises gain a comprehensive view of user behavior and activities across their entire enterprise cloud environment from a single user interface.

UBA is just one of many capabilities available in Oracle CASB Cloud Service. Delivering cloud security automation, the platform offers a holistic view of threats across business-critical cloud services. Such an approach is critical for enterprises to detect cross-cloud threats, ensure compliance, and respond to incidents in most efficient manner.

KEY CAPABILITIES

Oracle CASB Cloud Service provides comprehensive visibility and security of your entire cloud environment. Key security features include:

- Graphical dashboard of risky users across all cloud applications
- Forensic, drill-down capability with detailed risk analysis
- Dynamic, user-risk scoring based on continual assessment of user behavior
- Detection of suspicious or risky behavior based on access patterns, administrative actions, and device characteristics
- Importation of user identity from a single sign-on solution to extend user correlation and threat detection
- Profiling of all users across all applications with single sign-on solution integration
- Integrated workflow, including placing surveillance on risky users
- Auto-remediation and denial of application access based on user risk scores with integrated single sign-on solution

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/oracle

twitter.com/oracle

oracle.com

FOR MORE INORMATION

Contact: 1.800.ORACLE1

ORACLE®

Integrated Cloud Applications & Platform Services